Finance

Phishing Attack on Cloud Provider With Fortune 500 Clients Led to $15M Crypto Theft From Fortress Trust

CoinDesk has identified the vendor, previously blamed but not named by Fortress for the theft that helped spur the trust company's deal to sell itself to Ripple.

By Nikhilesh De, Marc Hochstein, Ian Allison Sep 13, 2023 at 4:37 p.m. EDT

Updated Sep 14, 2023 at 12:05 p.m. EDT

When Fortress Trust disclosed a theft of customers' cryptocurrency last week – later revealed to total close to $15 million – it pinned the blame on an unnamed third-party vendor.

CoinDesk has identified that vendor, which has acknowledged it fell victim to a phishing attack. But the story may be more complicated than just a single party's blunder.

The vendor is Retool, a San Francisco-based company with Fortune 500 customers, which built the portal for a handful of Fortress clients to access their funds, people familiar with the matter said.

The theft, which helped spur Fortress to agree to sell itself to blockchain tech company Ripple, occurred as a result of a phishing attack, they said.

When asked to comment, Retool referred CoinDesk to a Wednesday blog post detailing – without naming Fortress – how it had notified 27 of its customers on Aug. 29 that "there had been unauthorized access to their accounts" as a result of a phishing attack.

The attackers targeted “a specific set of customers,” all of whom were in the crypto business. However, Retool said customers that configured its software the way it “encourage[s]” them to consider doing (“if security is important”) were not affected, and that the vast majority of crypto customers use the product that way.

“We’re glad that not a single on-premise Retool customer was affected. Retool on-prem operates in a ‘zero trust’ environment, and doesn’t trust Retool cloud,” the blog post said. “It is fully self contained, and loads nothing from the cloud environment. This meant that although an attacker had access to Retool cloud, there was nothing they could do to affect on-premise customers. It’s worth noting that the vast majority of our crypto and larger customers in particular use Retool on-premise.”

Even though customers have been made whole, the theft from Fortress customers has been the talk of Crypto Twitter this week, with industry leaders pointing fingers at each other and several prominent companies caught up in the affair. But Retool’s role in the affair has not previously been reported.

Crypto vulnerabilities

The situation highlights a challenge that the cryptocurrency market, the way it has evolved, faces along with the traditional finance industry: There are numerous potential points of vulnerability, and problems often crop up because of some unexpected flaw somewhere in the system.

While $15 million is not an insignificant sum, it is a relatively small percentage of the billions of dollars worth of overall assets that Ripple says Fortress holds on customers' behalf. To help Fortress make customers whole, Ripple has made a $15 million “down payment” on its yet-to-close acquisition of the Nevada-based trust company, one person with direct knowledge of the situation said. The payment is a small fraction of the total purchase price, this person said.

A Ripple spokesperson said Fortress covered most of the affected customers but Ripple “stepped in to make the rest of those customers whole,” and all customers were covered within a week.

Theft ‘accelerated’ M&A talks

Fortress disclosed the security incident in a tweet on Sept. 7, but did not identify the “third-party vendor” whose cloud tools it said were compromised. The Nevada trust company stated at the time that there had been “no loss of funds.”

The next day, Ripple, which was already a minority investor in Fortress, announced it had signed a letter of intent to buy the custodian outright.

The companies were already in takeover talks when the theft occurred, but the incident accelerated them, a spokesperson for Ripple told CoinDesk in a statement on Monday.

“Conversations accelerated last week following the security incident via a third-party analytics vendor, but this opportunity makes sense for Ripple in the long term,” the statement said. “Luckily, Ripple was in a position to act quickly to step in and make customers whole, and there have been no breaches to Fortress technology or systems.”

Fortune reported the size of the theft to be in the range of $12 million to $15 million earlier Wednesday, citing Fortress co-founder and CEO Scott Purcell.

BitGo, Fireblocks, Swan

Fortress used wallets provided by Fireblocks and BitGo, neither of which were themselves breached, according to all three companies.

"The breach happened outside of the Fireblocks’ platform,” the company, known for using multi-party computation tools, told CoinDesk in a statement. “Due to Fireblocks’ key management system, authorization and policy engines, the size and reach of the impact on customer funds were drastically limited and customer funds were promptly restored.”

Mike Belshe, the CEO of BitGo, emphasized that the breach “has nothing to do with” his company in a tweet that criticized Fortress for its handling of the affair. (Fortress co-founder, Chief Technology Officer and Chief Product Officer Kevin Lehtiniitty responded to those criticisms in a tweet of his own.)

Swan Bitcoin, a brokerage firm that uses Fortress' BitGo wallets to hold client funds, said in a tweet that the coins stored there "did not move during the reported incident at Fortress. The coins are protected by video calls and physical access, and are not subject to any incidents at Fortress."

The Nevada Financial Institutions Division, the state regulator overseeing Fortress, was notified of the incident on Sept. 1, an agency spokesperson told CoinDesk.

Helene Braun contributed reporting.

STORY CONTINUES BELOW

Recommended for you:

- EU Parliament Approves Data Act With Smart-Contract Kill Switch Provision
- What Is a Crypto Exchange Token and How Did It Help Blow up FTX?
- Bitcoin Fund Holdings Hit All-Time High as Spot ETF Excitement Entices Crypto Investors

---

UPDATE (Sept. 14, 16:03 UTC): Adds attribution to size of Fortress' assets under management.

Edited by Nick Baker.

DISCLOSURE

Please note that our privacy policy, terms of use, cookies, and do not sell my personal information has been updated.

The leader in news and information on cryptocurrency, digital assets and the future of money, CoinDesk is a media outlet that strives for the highest journalistic standards and abides by a strict set of editorial policies. CoinDesk is an independent operating subsidiary of Digital Currency Group, which invests in cryptocurrencies and blockchain startups. As part of their compensation, certain CoinDesk employees, including editorial employees, may receive exposure to DCG equity in the form of stock appreciation rights, which vest over a multi-year period. CoinDesk journalists are not allowed to purchase stock outright in DCG.

Nikhilesh De

Nikhilesh De is CoinDesk's managing editor for global policy and regulation. He owns marginal amounts of bitcoin and ether.

Follow @nikhileshde on Twitter

Marc Hochstein

Marc Hochstein is the executive editor of Consensus, CoinDesk's flagship event. He holds BTC above CoinDesk's disclosure threshold of $1K and de minimis amounts of other digital assets (details on profile page).

Follow @MarcHochstein on Twitter

Ian Allison

Ian Allison is an award-winning senior reporter at CoinDesk. He holds ETH.

Follow @IanAllison123 on Twitter